ASSIGNMENT 3

Textbook Assignment: "Communications Administration (continued)," chapter 2, pages 2-29 through 2-37; "Communications, Security," chapter 3, pages 3-1 through 3-12; "AIS Security," chapter 4, pages 4-1 through 4-12.

3-1. If you desire to delete an existing DCS circuit, you should submit what type of request?

1. An AUTODIN deletion request
2. A telecommunications service request
3. A DCA circular request
4. A technical control service request

3-2. Requirements for new telecommunications services should be defined and submitted what minimum time in advance?

1. 1 yr
2. 2 yr
3. 3 yr
4. 6 mo

3-3. What does a TSO authorize?

1. Funding to begin basic circuit design
2. Starting, changing, or discontinuing circuits
3. Procurement of specific devices or ancillary equipment
4. Both 2 and 3 above

3-4. Navy funds cannot be obligated for developing or procuring communications equipment that uses a portion of the frequency spectrum until what is obtained?

1. Frequency usage estimate
2. A frequency allocation
3. A spectrum study
4. An FCC recommendation

3-5. Which of the following constraints should be considered when a frequency assignment is authorized?

1. Power, emission bandwidth, location of antennas, and operating time
2. Power, receiver locations, and atmospheric conditions
3. Bandwidth, sidebands, harmonics, and power requirements
4. Power, harmonics, and RF hazards to personnel

3-6. What authority grants Navy and Marine Corps activities within the U.S. permission to use radio frequencies?

1. Naval Electromagnetic Spectrum Center (NAVEMSCEN)
2. National Telecommunications and Information Administration (NTIA)
3. United States Military Communications Electronics Board (USMCEB)
4. Chief of Naval Operations (CNO)

3-7. In the Navy, what organization authorizes frequency assignment applications?

1. The United States Military Communications Electronics Board (USMCEB)
2. The National Telecommunications and Information Administration (NTIA)
3. The Joint Chiefs of Staff
4. The Naval Electromagnetic Spectrum Center (NAVEMSCEN)

3-8. Who is authorized to send PERSONAL FOR messages?

1. E-7 military or GS-7 civilian (or above)
2. Officers of flag rank or in a command status only
3. All officers
4. Anyone who needs to send a personal message

3-9. What is contained in the publications in the NWPL?

1. Manning plans, battle organizations, and future deployment schedules
2. Awards information, maintenance schedules, and supply information
3. Required procedures, signals, and other operational and mission-essential information
4. Operational requirements, battle organizations, and deployment schedules

3-10. What is the objective of the central administration of the NWPL?

1. To ensure that the publications in the NWPL are correct and readily avail-able for use
2. To ensure that personnel have a place to study for advancement
3. To ensure that personnel have access to publications and periodicals on the latest technology
4. To ensure that personnel have access to the most recent and best-selling novels

3-11. Who is responsible for the management of the NWPL?

1. The naval warfare publications officer
2. The naval warfare publications custodian
3. The naval warfare publications librarian
4. The naval warfare publications manager

3-12. What publication provides guidance for the administration and security of the NWPL?

1. OPNAVINST 5510.1
2. NTP 4
3. NWP 4 (NWP 6-01)
4. NWP 0 (NWP 1-01)

3-13 . Who is responsible for changes or corrections to NWPL publications?

1. The NWPL clerk
2. The primary user
3. The NWPL custodian
4. The communications watch officer

3-14. Who is considered to be a holder under the administration of NWPL?

1. A person who holds NWPL publications for short terms only
2. A person who transports publications to and from the NWPL
3. A person who has permanent subcustody of publications from the NWPL
4. The NWPL custodian

3-15. Which of the following files are used in NWPL maintenance?

1. Signature and custody fries
2. Administrative and transaction files
3. Signature and administrative files
4. Custody and administrative files

3-16. The NWPL administrative file is also known by what other term?

1. Transaction file
2. Office file
3. A-1 file
4. Custody file

3-17. Material in the administrative file must be retained for what minimum time ?

1. 1 yr
2. 2 yr
3. 5 yr
4. 6 mo

3-18. What colors are assigned to the binders for U.S. naval warfare publications of different classifications?

1. Secret - red, Confidential - green, Unclassified - white
2. Secret - red, Confidential - yellow, Unclassified - blue
3. Secret - red, Confidential - yellow, Unclassified - white
4. Secret - red, Confidential - green, Unclassified - blue

3-19. Where is the effective date of the publication change/correction found?

1. In the Record of Changes page
2. In the List of Effective Pages (LOEP)
3. In the Foreword or Letter of Promulgation
4. In the Title page

3-20. Which of the following colors should be used to make pen-and-ink corrections to NWPL publications?

1. Green only
2. Black or blue only
3. Any dark color except red
4. Any color is acceptable

3-21. What does the designation "NMC 6/2" on a correction mean?

1. It is the 6th message correction and will-be incorporated into the publication by printed change number 2
2. It is the 2nd message correction and will be incorporated into the publication by printed change number 6
3. It was sent on the 2nd of June of the current year
4. It is the 6th change to the 2nd revision of the publication

3-22. What document contains guidance for taking extracts from a NATO publication?

1. OPNAVINST 5510.1
2. ACP 121
3. NWP 0 (NWP 1-01)
4. NATO letter of promulgation

A. ACPs
B. NTPs
C. JANAPs
D. NWPs

Figure 3A

IN ANSWERING QUESTIONS 3-23 THROUGH 3-26, SELECT THE PUBLICATIONS FROM FIGURE 3A THAT ARE DESCRIBED.

3-23. Provide communications instructions and procedures essential to conducting combined military operations in which two or more allied nations are involved.

1. A
2. B
3. C
4. D

3-24. Coordinate and standardize communications procedures among U.S. military services.

1. A
2. B
3. C
4. D

3-25. Main publications used by Navy, Coast Guard, and Marine personnel for communications.

1. A
2. B
3. C
4. D

3-26. Incorporate the results of fleet tactical development and evaluation programs and NATO experience and provide information about the tactical capabilities and limitations of equipment and systems.

1. A
2. B
3. C
4. D

A. CMS account
B. CMS custodian
C. CMS local holder
D. CMS user

Figure 3B

IN ANSWERING QUESTIONS 3-27 THROUGH 3-29, SELECT THE TERM FROM FIGURE 3B THAT IS DESCRIBED.

3-27. A command with an account number that draws its COMSEC material directly from national or Navy distribution sources.

1. A
2. B
3. C
4. D

3-28. COMSEC material needs are met by drawing such material from the squadron commander.

1. A
2. B
3. C
4. D

3-29. An individual who requires the use of COMSEC material for a short time to accomplish a specific task.

1. A
2. B
3. C
4. D

3-30. Which of the following statements concerning storage requirements for COMSEC material is/are correct?

1. COMSEC material may be stored with other communications material according to security classification
2. COMSEC material must be stored separately from non-COMSEC material
3. COMSEC material of different classification may be stored. together regardless of classification if storage limitations are a factor
4. Both 2 and 3 above

3-31. What number of signatures is/are required on the COMSEC watch-to-watch inventory sheet?

1. One
2. Two
3. Three
4. Four

3-32. What is the maximum length of time that you are authorized to hold superseded (a) keying material marked CRYPTO and (b) authentication publications?

1. (a) 24 hours (b) 24 hours
2. (a) 12 hours (b) 5 days
3. (a) 5 days (b) 12 hours
4. (a) 5 days (b) 5 days

3-33. What are the three types of keying material in descending priority of destruction?

1. Superseded, reserve, effective
2. Effective, superseded, reserve
3. Reserve, effective, superseded
4. Superseded, effective, reserve

3-34. Effective keying material is the most sensitive of the three types of keying material.

1. True
2. False

3-35. What is the purpose of Two-Person Integrity?

1. To prevent a single person from having access to COMSEC material
2. To prevent more than two persons from having access to COMSEC material
3. To provide for an alternate custodian in the event the primary is unavailable
4. To allow for a division of responsibilities among the custodians

A. CRYPTO
B. Cryptoinformation
C. Crypto-related information
D. Cryptosystem

Figure 3C

IN ANSWERING QUESTIONS 3-36 THROUGH 3-39, SELECT THE TERM FROM FIGURE 3C THAT IS DESCRIBED.

3-36. Marking used to protect or authenticate national security-related information on all keying material and associated equipment.

1. A
2. B
3. C
4. D

3-37. Always classified and normally concerns the encryption or decryption process of a cryptosystem.

1. A
2. B
3. C
4. D

3-38. May be classified or unclassified; normally associated with cryptomaterial but not significantly descriptive of it.

1. A
2. B
3. C
4. D

3-39. Encompasses all associated items of cryptomaterial that provide a single means of encryption and decryption.

1. A
2. B
3. C
4. D

3-40. A failure that adversely affects the security of a cryptosystem is known by what term?

1. Cryptoexposure
2. Cryptoinstability
3. Cryptodeficiency
4. Cryptoinsecurity

3-41. A system within a general system confined to actual encryption, decryption, or authentication is known by what term?

1. Cryptovariable
2. Specific cryptosystem
3. Secondary cryptosystem
4. Supporting cryptosystem

3-42. The most frequently changed element of a cryptosystem is known by what term?

1. Primary cryptovariable
2. Secondary cryptovariable
3. Crypto modifier
4. Cryptosystem internal variable

3-43. What are the primary advantages of (a) over-the-air rekey (OTAR) and (b) over-the-air transfer (OTAT)?

1. (a) Requires less circuit downtime for loading keylists, and (b) no operator training required
2. (a) Reduces distribution of physical keying material, and (b) eliminates process of loading equipment with key tapes
3. (a) Reduces distribution of physical keying material, and (b) no operator training required
4. (a) Eliminates process of loading equipment with key tapes, and (b) no operator training required

3-44. What is the purpose of transmission authentication?

1. To guard against fraudulent or simulated transmissions
2. To inform the other operator that you are receiving the transmission
3. To acknowledge the transmission of the other operator
4. To allow the other operator to acknowledge your transmission

3-45. The self-authentication method is used in which of the following transmissions?

1. Transmission and reply
2. Challenge and reply
3. Transmission authentication
4. Challenge authentication

3-46. When you receive a message that has an authenticator in it, what action, if any, are you required to take?

1. Prepare a message to challenge the originator
2. Send a message that you are in receipt of the message
3. Pass the message on to higher authority for them to challenge the originator
4. None

3-47. As an operator, you are required to authenticate in which of the following situations?

1. You suspect intrusion on the circuit
2. You are requested to authenticate
3. You are requested to break radio silence
4. Each of the above

A. Meaconing
B. Interference
C. Jamming
D. Intrusion

Figure 3D

IN ANSWERING QUESTIONS 3-48 THROUGH 3-51, SELECT THE TERM FROM FIGURE 3D THAT IS DEFINED.

3-48. The interception and rebroadcast of navigational signals on the same frequency.

1. A
2. B
3. C
4. D

3-49. An attempt by the enemy to enter U.S. or allied communications systems and simulate traffic with the intent to confuse and deceive.

1. A
2. B
3. C
4. D

3-50. The deliberate use of electromagnetic signals with the objective of impairing communications circuits.

1. A
2. B
3. C
4. D

3-51. Usually a nondeliberate electrical disturbance that unintentionally prevents the effective use of a frequency.

1. A
2. B
3. C
4. D

3-52. Which of the following statements best describes the overall goal of AIS security?

1. To take all reasonable measures to protect AIS assets
2. To prevent data and programs from being destroyed or sabotaged
3. To keep unauthorized personnel out of your AIS facility
4. To take whatever measures are necessary to protect equipment and people

3-53. Which of the following assets is NOT considered an AIS asset?

1. People
2. Hardware
3. Software
4. Environment

3-54. In AIS security terminology, what term is used for the things that can destroy AIS assets?

1. Threats
2. Probability
3. Vulnerability
4. Countermeasures

3-55. To express the cost of a loss or abuse from an adverse event over time, what AIS security term is used?

1. Risk
2. Likelihood
3. Vulnerability
4. Countermeasure

3-56. In AIS security, risks are usually expressed in which of the following terms?

1. Days
2. Dollars
3. Equipment
4. Personnel

3-57. In AIS security terminology, the controls to lessen or eliminate known threats and vulnerabilities are called

1. physical barriers
2. security routines
3. backup procedures
4. countermeasures

3-58. Under AIS security, countermeasures (controls) that are embedded in hardware, software, and telecommunications equipment are what type of controls?

1. Physical
2. Technical
3. Managerial
4. Administrative

3-59. Under AIS security, countermeasures (controls) that concern people and procedures, such as who is authorized to do what or who receives or requests a sensitive report, are what type of controls?

1. Physical
2. Technical
3. Managerial
4. Administrative

3-60. Under AIS security, countermeasures (controls) that concern planning and evaluation, such as audits to review the effectiveness and efficiency of countermeasures that are in place, are what type of controls?

1. Physical
2. Technical
3. Managerial
4. Procedural

3-61. In regard to AIS security, the continuation of an activity's mission during abnormal operating conditions is provided by which of the following means?

1. Countermeasures
2. Contingency plans
3. Security risk plan
4. Emergency response team

3-62. In addition to hardware and software, what are the other three areas of consideration for the Navy's AIS security program?

1. Data, personnel, and environment
2. Data, human resources, and logistics
3. Data, human resources, and communications
4. Media libraries, environment, and communications

3-63. Which of the following personnel serves as the single point of contact for all matters related to AIS security?

1. Executive officer
2. Information system security manager
3. Security violations officer
4. Systems security manager

3-64. AIS security is not really that difficult to understand. What percent is (a) common sense, and (b) proper training?

1. (a) 55% (b) 45%
2. (a) 60% (b) 40%
3. (a) 65% (b) 35%
4. (a) 70% (b) 30%

3-65. The manufacturer's optimum temperature and humidity range specifications for AIS equipment operation are NOT available. Which of the following (a) temperature and (b) humidity ranges are considered acceptable for computer operation?

1. (a) 65° ±5° (b) 55% ±5%
2. (a) 65° ±5° (b) 65% ±2%
3. (a) 72° ±2° (b) 55% ±5%
4. (a) 72° ±2° (b) 65% ±2%

3-66. In AIS environmental security, emergency lights are installed in computer facilities for what primary reason?

1. To protect personnel
2. To assist fire fighters
3. To locate AIS equipment
4. To locate fire-fighting equipment

3-67. Fluctuations in electrical power can adversely affect the operation of AIS equipment. If your command's mission dictates continuous AIS support, each computer system should be equipped with which of the following equipment?

1. A motor/generator
2. An ac, dc regulator
3. A voltage surge protector
4. An uninterrupted power source

3-68. In regard to AIS security, master control switches are used to shut off all power to your AIS spaces in the event of a fire. These master control switches are normally installed at what location?

1. In the CO^2 storage room
2. In the security officer's space
3. At the exit doors of the AIS spaces
4. On the master control panel of the computer

3-69. Which of the following security modes does NOT apply to processing classified or level I data?

1. Dedicated
2. System low
3. Multilevel
4. System high

3-70. For processing classified, the central computer facility and all its related peripheral devices (both local and remote) are protected for the highest classification category and type of material contained in the system. The system is said to be in what security mode?

1. Controlled
2. System low
3. System high
4. Totally dedicated

3-71. For processing level I data, the central computer facility and all its related peripheral devices (both local and remote) are exclusively used and controlled by specific users having a security clearance and need-to-know for the processing of a particular cateqory of classified material. The system is operating in what security mode?

1. Dedicated
2. System low
3. Multilevel
4. System high

3-72. For processing level I data, an AIS system provides the capability of permitting various categories of classified materials to be stored, processed, and selectively accessed on a concurrent basis by users having differing clearances and need-to-know. The system is said to be in what security mode?

1. Controlled
2. Undedicated
3. System low
4. Multilevel

3-73. What category of AIS media is considered temporary in nature and is retained for 180 days or less?

1. Smooth
2. Working
3. Finished
4. Intermediate

3-74. Which of the following categories of AIS media is permanent in nature and is retained for a period of more than 180 days?

1. Smooth
2. Working
3. Finished
4. Intermediate